TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Arvutiteaduse instituut

Võrgutarkvara õppetool

Autoarvuti ründed ning vastumeetmed

Referaat

Üliõpilane: Andri Rebane

Üliõpilaskood: 020505

Tallinn

2008

Sisukord

1. Sissejuhatus

Antud töös on vaadeldud arvuti kasutamise piiratud erijuhtu – autoarvuti, mis on vajalik interaktiivsete teenuste (ID-tuvastus, positsioneerimine, reaalajas info vahetamine keskse serveriga) pakkumiseks autos ning sellega seonduvates teenustes (autos kogutavad andmed töödeldakse, luues lisaväärtust).

1.1. Autoarvuti eripärad

Autoarvuteid on mitmeid erinevaid tüüpe, neist lihtsamad on moodulipõhised seadmed, mille ainukesteks ülesanneteks on GPS andmete kogumine ning kesksele serverile saatmine. Nende eeliseks on lihtsus, odavus ning väike voolutarbimine, mis võimaldab neil töötada ja andmeid saata ka siis kui auto mootor ei tööta. Samuti on neid raskem rünnata, kuna tegemist on erilahendustega ning puuduvad sagedamini rünnatavad programmid (näiteks operatsioonisüsteem).

Antud töös käsitletud arvutiks on Windows XP põhine PC tüüpi mini-ITX mõõdus arvuti, mis on valitud lisafunktsionaalsuste tõttu, mida moodulipõhine arvuti ei võimalda – mitme ID-kaardi kasutamine, Google Maps rakenduse kasutamine positsioneerimiseks, monitori veebi kasutamiseks, video salvestamine jne. Antud funktsionaalsuste tõttu on autoarvuti kordades avatum erinevatele rünnetele ning vajab seetõttu erinevaid lähenemisi turvalisuse tõstmiseks.

2. GPS seadme ründed

GPS seadmeks on antud projekti puhul seade Globalsat BU-353 SiRFStarIII kiibistikuga, ühendudes arvuti külge USB-ga ning emuleerides COM porti (USB-to-serial). Teadaolevalt puuduvad otsesed ründevõimalused antud riistvara suhtes, mis võimaldaksid lokaalses arvuti piires seadme väljundit pahatahtlikult muuta.

2.1. Segamine

Segamine (jamming) on kõige lihtsam ning odavam viis muuta GPS seade töövõimetuks. GPS-signaali segaja eesmärgiks on segada GPS seadmel signaali saamist GPS satelliitidelt ning sellega takistada sõiduki asukoha määramist.

GPS-signaali segajate hinnad algavad 40 dollarist, nad on äärmiselt kompaktsed (pikkus alla 10 cm). Odavad segajate tüübid:

- 12V seadmed, mis võtavad voolu auto sigaretisüütajast, moodustavad, segava signaali võimsuseks on ca 200 mW ning nende võimalus segada on 5-15m raadiuses. Seega piisab sellest tavalises sõiduautos signaali segamiseks ning võimaldab kurjategijatel autoga peidupaika sõita.
- Patareitoitel seadmed, mille segav signaal algab samuti 200mW ning moodustavad seadme ümber alates 5m suuruse segava signaali. Võimaldab GPS signaali segada juba enne autosse sisenemist või segada signaali sõidu pealt.
- Inverteriga seadmed, mille väljundvõimsus ulatub 6.5W ning üle selle, võimaldab luua üle 40m raadiusega segavad ala, võimaldades rünnatavat objekti sõidu pealt segada.

Kindlasti on võimalik soetada ning ise ehitada veelgi võimsamaid seadmeid, mis võimaldaksid GPS signaali märkamatult kaugusest segada.

2.2. Satelliitide väärinfo

Teadaolevalt on GPS süsteem USA Kaitseministeeriumi poolt loodud ning hallatav, sellega seoses on kõik GPS süsteemi kasutajad otseselt sõltuvad seda süsteemi haldava asutuse tööst. GPS signaali on võimalik ajutiselt või püsivalt muuta ebatäpseks (praeguselt ühelt meetrilt sajale meetrile ja rohkem) või teatud piirkonna kasutajaid eksitada, nagu on seda ka Eestis täheldatud USA presidendi siin viibimise ajal (1). Tõenäosus, et antud rünnet kasutatakse konkreetselt autoarvutite ründamiseks või eksitamiseks on siiski äärmiselt ebatõenäoline.

2.3. GPS müüdid seotud ründamisega

- Halb ilm segab märkimisväärselt GPS signaali vastuvõttu, seetõttu puudub vastuvõttev signaal GPS seadmel – GPS signaali sagedus on valitud nii, et pilved, vihm jms loodusnähtused segavad seda minimaalselt. Kui auto esiklaasil olev GPS seade võtab vihmaga signaali kehvemini vastu, siis pigem on tegu kojameestest tuleneva signaali nõrgenemisega kui vihmast. Seega viitab pikaajaline signaali puudumine pigem segaja olemasolule lähipiirkonnas.
- GPSi abil on võimalik läbi viia jälgimist, selle kaudu tuvastada kasutaja asukohta – jälgimist on võimalik läbi viia vaid siis kui seadmel on ka mingit sorti tagasiside võimekus. Tavaline GPS seade suudab signaali vaid vastu võtta ning paremal juhul (mitte kõik mudelid) seda mõnda teise seadmesse edasi anda.

3. Mobiilse seadme ründed

Mobiilseks seadmeks autoarvuti küljes on antud projekti raames GPRS/UMTS modem Huawei E220, mis ühendub arvutiga USB pesa kaudu ning emuleerib COM porti (USB-to-serial) andmete vahetamiseks.

3.1. Mobiilse seadme firmware muutmine

Modemile Huawei E220 on ette nähtud ametlikud firmware uuendused, mis peaksid seadme tööd parandama. Samas ei ole välistatud pahatahtlike uuenduste levik ning seadmele sattumine, mille puhul oleks võimalik kogu liiklust pealt kuulata, koguda ning vastavalt vajadusele muuta.

Samuti oleks võimalik seadmele lisada pahavara, mis leviks sarnaselt mälupulkadel levivate viirustega.

3.2. Segamine

Sarnaselt GPS segamise seadmetele, hakkavad ka GSM sageduse segajate hinnad mõnekümnest dollarist, taskukohased seadmed on võimelised korraga segama nii USA kui ka Euroopa sagedusi, nii saatvaid, kui ka vastuvõtvaid sagedusi. Segajate tööraadius algab taas mõnest meetrist ümber seadme, ulatudes kilomeetriteni vastavalt segaja võimsusele.

Parimaid tulemusi saavutatakse nö „combo“ seadmetega, mis on üheaegselt võimelised segama nii GPS kui ka GSM signaali

3.3. Võrguliikluse pealtkuulamine ning võltsimine (Man in the Middle Attack)

Kuna GPRS on suuresti üles ehitatud GSM standarditele, siis on mõned selle turvaaugud kandunud edasi ka GPRS ühendusele. GPRS kasutab andmeühenduseks IP-d, mille loomise ajal polnud turvalisus eesmärgiks. Samuti on GPRS võrgus võimalikud Man in the Middle ründed (2).

4. Arvuti ründed

4.1. Arvuti füüsiline rünne

Autoarvuti on suhteliselt kaitsetu füüsilise ründe vastu:

- Autod seisavad sageli valveta asukohtades ning on lihtne jõuda füüsiliselt arvutini.
- Arvutil on aktiivsed USB pesad, mis on vajalikud lisaseadmete tööks, seega on võimalik nende kaudu sisestada arvutisse pahavara.
- Arvutil puuduvad krüpteeritud andmekandjad (ajapuudusel testimata, võimalik kasutada näiteks TrueCrypt krüpteerimistarkvara), mis võimaldab ründajal enda valdusesse saada seal paiknevad andmed.

4.2. Arvuti operatsioonisüsteemi

Arvuti operatsioonisüsteemiks on Windows XP Home, mis on levinud operatsioonisüsteem paljude turvavigadega, milledele ei paista lõppu olevat. Kuna autoarvuti Internetiühenduseks on GPRS, mille kuine andmemaht on piiratud 3GB-ga, on keelatud operatsioonisüsteemi uuenduste automaatne allatõmbamine ja installeerimine, mis omakorda tähendab, et kriitilised turvaaugud jäävad operatiivselt parandamata ning kuni järgmise manuaalse uuendamiseni on arvuti antud turvavigadest tulenevatele rünnetele avatud.

4.3. Arvuti tarkvara rünne

Arvuti rakendustarkvara on kirjutatud Javas, tegemist on üsna lihtsa programmiga, millel suure tõenäosusega puuduvad turvaaugud või on nende otsimine liialt kulukas võrreldes tuludega, mis ründest saadakse.

Muid rakendustarkvarasid (Office, pilditöötlusprogrammid, suhtlusprogrammid jms) arvutisse installeeritud ei ole ning kasutajale pole antud ka administraatori õigusi nende installeerimiseks.

5. Kaitse rünnakute vastu

5.1. Kaitse segamise vastu

Segamise vastu kaitse puudub, kuna eeldab omakorda segaja signaali segamist, mis omakorda takistaks enda signaali levimist. Ainukese lahendusena oleks ebatavalise sageduse kasutamine andmeedastusel (lisaks GPRS'ile on võimalik kasutada ka tavaliselt Wifit (sagedusel 2,4GHz) või Kõu seadmeid (sagedusel 400MHz).

5.2. Võrguliikluse krüpteerimine autoarvuti ja serveri vahel

Andmed, mis liiguvad autoarvuti ning serveri vahel on krüpteeritud piisavalt turvalise võtmega, mis tagab andmete turvalisuse ning võltsimatuse.

5.3. Arvuti varustamine turvatarkvaraga / tarkvara uuendamine

Autoarvuti on varustatud antiviiruse ning tulemüüritarkvaraga, mida uuendatakse igapäevaselt ning mis lubab siseneda vaid loodud ühendustel (server ei võta kunagi ise autoarvutiga ühendust, ühenduse algatajaks on autoarvuti).

5.4. Võrguliikluse piiramine

Autoarvuti GPRS ühendust looval programmil on võimalik seadistada võrguliikluse kalkulaator, mis teatud limiidi ületamisel sulgeb Internetiühenduse. Kuna teenusepakkuja mõistlikku kasutamise piir on 3GB andmemahtu kuus, siis sellega on piiratud ka autoarvuti Internetiliiklus. Antud lähenemine ei võimalda näiteks botnet ohvriks langenud autoarvutil tekitada rohkem kahju kui 3GB võrguliikluse väärtuses (jäävad ära DDoS ründed, laiaulatuslikud võrgu skanneeringud järgmiste ohvrite leidmiseks jms läbi autoarvuti).

6. Ründepuu

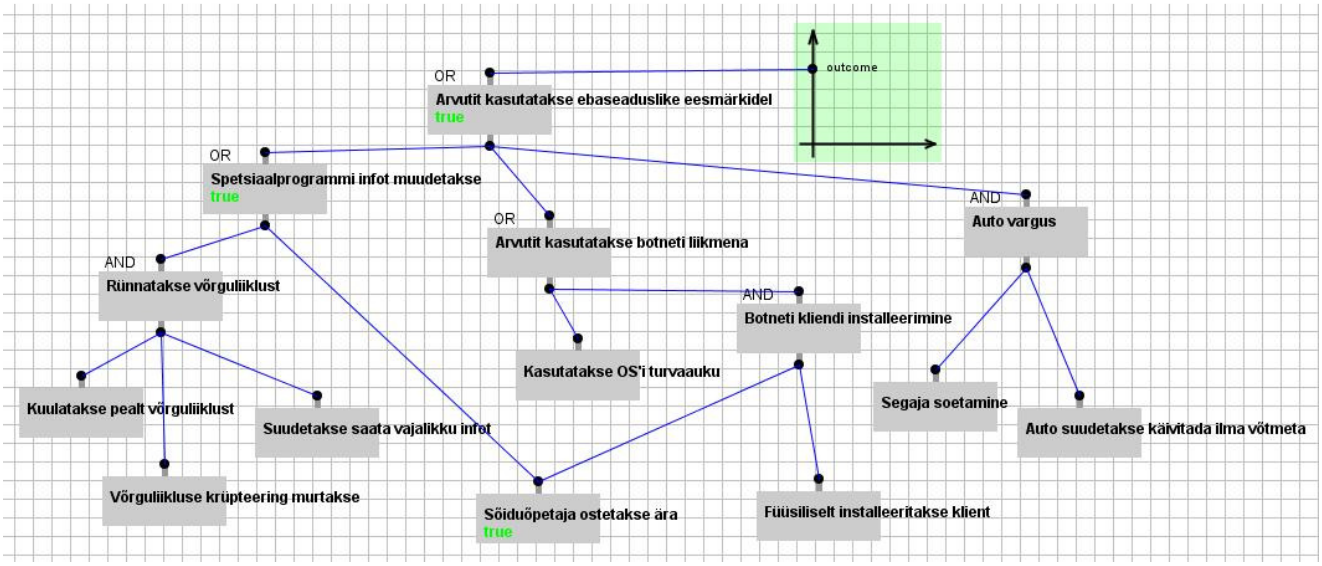
Et hinnata riske, et autoarvutit kasutatakse ebaseaduslikel eesmärkidel, sai loodud ründepuu programmiga Cocovila, paketiga SecTree. Ründepuu on äärmiselt subjektiivne, võivad puududa ründeharud ning olemasolevad ei pruugi vastata reaalsetele olukordadele, kuid siiski annab puu üldise ülevaate riskide hindamiseks.

Kasutatud on järgmisi andmeid:

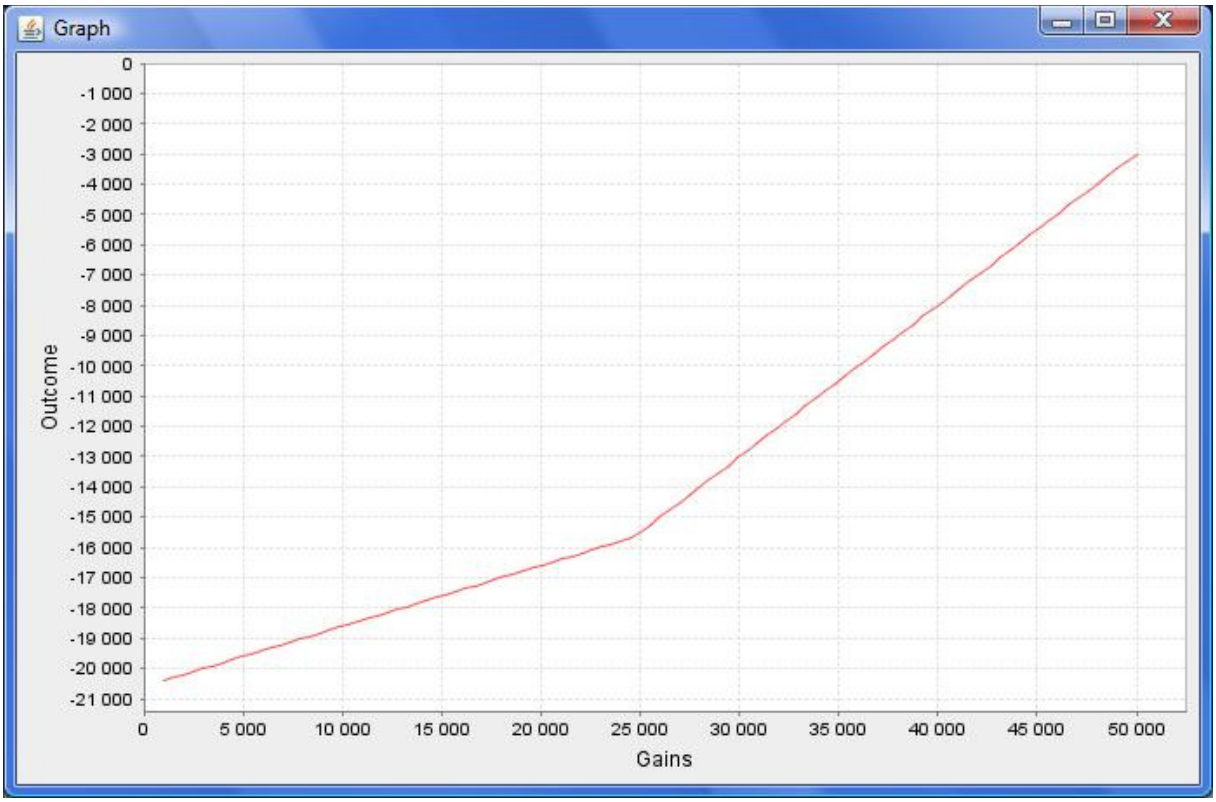
- Kõikvõimalike ebaseaduslike tegude eest on ette nähtud karistus kuni 18000 kr, muid karistusi (kinnipidamine, vanglakaristus jms) ei ole arvestatud.
- Tulemusena on arvestatud, et minimaalseks ründe eesmärgiks on 1000 kroonise kasu saamine (andmete muutmine rahalises väärtuses) ning maksimaalselt 50000 kr kasu saamine (auto vargusest saadav tulu).
- Andmetabel:

Rünne	Maksumus	Ründe edukuse tõenäosus	Karistus kui rünne õnnestub	Karistus kui rünne ebaõnnestub
Kuulatakse pealt võrguliiklust	20000	0.7	18000	18000
Võrguliikluse krüpteering murtakse	50000	0.1	18000	18000
Suudetakse saata vajalikku infot	3000	0.95	6000	6000
Sõiduõpetaja ostetakse ära	10000	0.5	3000	3000
Kasutatakse operatsioonisüsteemi turvaauku	3000	0.3	6000	6000
Füüsiliselt installeeritakse botnet klient	1000	0.9	3000	3000
Segaja kasutamine	1000	1.0	18000	18000
Auto käivitatakse ilma originaalvõtmeta	10000	0.3	18000	18000

- Ründepuu graafiliselt:



- Ründepuu tulemuse graafik:



Graafikult võib näha, et auto süsteemide ründamine kasu eesmärgil ei tasu ära, kuna kulutused ja risk on suuremad kui nendest saadav tulu. Graafiku murdepunkt näitab tasuvuse üleminekut operatsioonisüsteemi turvaaugu ründest sõiduõpetaja ära ostmiseks, mis tähendab, et kõige

ohtlikum element kogu süsteemis on endiselt töötaja, kelle tekitatud kahjud võivad sageli olla suuremad kui rünnetel, kus sisemist infot kasutada pole võimalik. Seega tasub mõelda kasutajaõiguste piiramisele ning minimaliseerimisele, õiguste pidevale kontrollile, samuti autoarvutis oleva spetsiaalprogrammi funktsionaalsuste piiramisele.

Kasutatud kirjandus

1. **Samuel, Tõnu.** minut.ee - Järelehüüe Bushile. [Võrgumaterjal] 28. 11 2006. a. [Tsiteeritud: 3. 10 2008. a.] http://www.minut.ee/article.pl?sid=06/11/28/1415212&mode=nested.

2. **Teadmata.** GPRS Security. [Võrgumaterjal] Teadmata. [Tsiteeritud: 06. 11 2008. a.] http://www.google.co.uk/history/url?url=http://dsns.csie.nctu.edu.tw/course/wireless_sec/2008/slide/6-2_GPRS.pdf&ei=JikTSYf8JIXo8QP95YiGBQ&sig2=-4O6R8O7p8KwdnVKqStPWg&ct=w.